(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
2. Juni 2005 (02.06.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/050911 A1

(51) Internationale Patentklassifikation[7]: H04L 9/32

(21) Internationales Aktenzeichen: PCT/EP2004/012995

(22) Internationales Anmeldedatum:
16. November 2004 (16.11.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 53 853.4 18. November 2003 (18.11.2003) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **WEISS, Dieter** [DE/DE]; Brucknerstrasse 25, 81677 München (DE). **RANKL, Wolfgang** [DE/DE]; Frauenalplweg 2, 81825 München (DE).

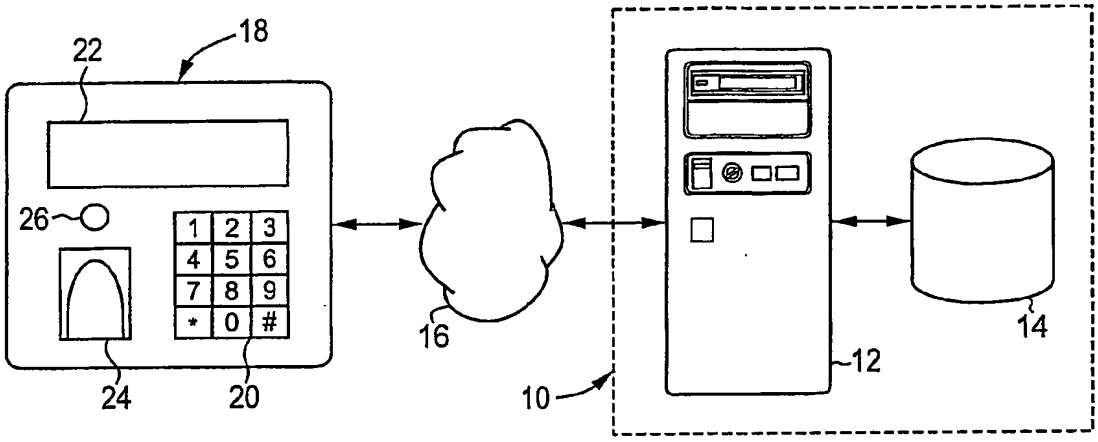
(74) Anwalt: **DENDORFER, Claus**; Wachtershäuser & Hartz, Weinstrasse 8, 80333 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG,

[Fortsetzung auf der nächsten Seite]

(54) Title: AUTHORISATION OF A TRANSACTION

(54) Bezeichnung: AUTORISIERUNG EINER TRANSAKTION



(57) Abstract: The invention relates to a method for the authorisation of a transaction by a user with the aid of a terminal (18) which can communicate with a background system (10). A secret, which is known to the user and to the background system (10) but not to an unauthorised person, is used. The background system (10) initially transmits the secret data, indicating the secret, to the terminal (18) when the terminal (18) has successfully been authorised by the background system (10). Secret data of several users are, as a rule, stored in the background system (10). The terminal (18) detects in advance identification information which identifies the user, and transmits corresponding user identification data to the background system (10). When the terminal (18) displays the secret to the user, the user can be certain that the terminal is (18) trustworthy. A device and a computer program product comprise corresponding characteristics. The invention also relates to a technique for the authorisation of a transaction by a user with the aid of a terminal (18) which enables the user to recognise a falsified terminal (18).

(57) Zusammenfassung: Bei einem Verfahren zur Autorisierung einer Transaktion durch einen Benutzer unter Verwendung eines Terminals (18), das mit einem Hintergrundsystem (10) zu kommunizieren vermag, wird ein Geheimnis verwendet, das dem Benutzer und dem Hintergrundsystem (10), nicht

[Fortsetzung auf der nächsten Seite]

WO 2005/050911 A1

PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Bestimmungsstaaten** *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärung gemäß Regel 4.17:

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO Patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

aber einem unbefugten Angreifer, bekannt ist. Das Hintergrundsystem (10) übermittelt Geheimnisdaten, die das Geheimnis angeben, erst dann an das Terminal (18), wenn sich das Terminal (18) erfolgreich bei dem Hintergrundsystem (10) authentisiert hat. Da in dem Hintergrundsystem (10) in der Regel Geheimnisdaten vieler Benutzer gespeichert sind, ermittelt das Terminal (18) vorab Identifikationsinformationen, die den Benutzer identifizieren, und überträgt entsprechende Benutzerbezeichnungsdaten an das Hintergrundsystem (10). Wenn das Terminal (18) dem Benutzer das Geheimnis anzeigt, kann der Benutzer sicher sein, daß das Terminal (18) vertrauenswürdig ist. Eine Vorrichtung und ein Computerprogrammprodukt weisen entsprechende Merkmale auf. Die Erfindung stellt eine Technik zur Autorisierung einer Transaktion durch einen Benutzer unter Verwendung eines Terminals (18) bereit, die dem Benutzer die Möglichkeit gibt, ein gefälschtes Terminal (18) zu erkennen.